



**FEDERAL PKI POLICY AUTHORITY**

**September 18, 2011 MEETING MINUTES**

**USPS Headquarters  
475 L'Enfant Plaza, SW  
Conference Room: 4841  
Washington, DC  
9:30 a.m. – 10:34 a.m.**

<b>09:30</b>	<b>Welcome, Opening Remarks &amp; Introductions</b>	<b>Deb Gallagher, Chair</b>
<b>09:50</b>	<b>Discuss / Vote on September, 13 2011 FPKIPA Minutes</b>	<b>Matt King</b>
<b>10:00</b>	<b>FPKI Certificate Policy Working Group (CPWG) Report</b> <ul style="list-style-type: none"><li><b>1. Review/Vote on FPKIPA Charter and By-Laws</b></li><li><b>2. Discussion/Nominations for FPKIPA Chair</b></li><li><b>3. Review/Vote on FBCA and FCPF LDAP Change Proposals</b></li><li><b>4. Status Update on Device Cert Change Proposal</b></li><li><b>5. Review/Update Status of CPWG Ongoing Initiatives</b><ul style="list-style-type: none"><li><b>a. Review/Update Status of draft Criteria and Methodology</b></li><li><b>b. CAB Forum Extend Validation Certificate Guidelines Proposal</b></li><li><b>c. Definition of CMS</b></li></ul></li></ul>	<b>Charles Froehlich</b>
<b>10:45</b>	<b>FPKI Management Authority (FPKIMA) Report</b>	<b>Darlene Gore</b>
<b>11:30</b>	<b>Other Agenda Items</b> <ul style="list-style-type: none"><li><i>o ICAM Update—Deb Gallagher</i></li><li><i>o If you cannot attend, please designate an alternate, a proxy or an enduring proxy for such situations.</i></li></ul> <p><i>Next FPKIPA meeting, November 8, 2011</i></p>	<b>Deb Gallagher</b>
<b>12:00</b>	<b>Adjourn Meeting</b>	<b>Deb Gallagher</b>

## A. ATTENDANCE LIST

### a. Voting Members

Organization	Name	T – Telephone P – In Person A – Absent
Department of Defense (DOD)	Mitchell, Debbie	T
Department of Energy (DOE)	Thomas, Michele	T
Department of Health & Human Services (HHS)	Slusher, Toby	P
Department of Homeland Security (DHS)	Miller, Tanyette (Proxy for Don Hagerling)	P
Department of Justice (DOJ)	Morrison, Scott	P
Department of State (State)	Frahm, Jarrod M.	P
Department of Treasury (Treasury)	Wood, Dan	T
Drug Enforcement Administration (DEA CSOS)	Briggs, Sherrod (Proxy for Chris Jewell)	T
Government Printing Office (GPO)	Hannan, John	T
General Services Administration (GSA)	Gallagher, Deb	P
National Aeronautics & Space Administration (NASA)	Wyatt, Terry	T
Nuclear Regulatory Commission (NRC)	Sulser, David	P
Social Security Administration (SSA)	Mitchell, Eric	A
United States Postal Service (USPS)	Stepongzi, Mark	P
United States Patent & Trademark Office (USPTO)	Kless, Patricia	T
Veterans Administration (VA)	Jurasas, Eric	T

## b. Observers

Organization	Name	T – Telephone P – In Person
FPKI MA Technical Liaison (Contractor, Protiviti)	Brown, Wendy	P
DoS (Contractor, ManTech)	Froehlich, Charles	P
GSA, FPKI MAFPKIMA PM	Gore, Darlene	P
SSA (Contractor)	Hardy, Amy	T
State (Contractor)	Jung, Jimmy	T
FPKIPA (Contractor, Protiviti)	King, Matt	P
FPKIMA (Contractor, Protiviti)	Kotraba, Matt	T
US Access (Contractor)	Lins, Andrew	T
Entrust	Moore, Gary	T
GSA (Contractor, Unisys)	Petrick, Brant	P
FPKIPA (Contractor, Protiviti)	Sonnier, Tiffany	P

## B. MEETING ACTIVITY

### Welcome, Opening Remarks & Introductions, Deb Gallagher, Chair

The Federal Public Key Infrastructure Policy Authority (FPKIPA) met at the USPS Headquarters located at 475 L'Enfant Plaza, SW CR4841 Washington, DC. Ms. Deb Gallagher, Chair, called the meeting to order at 9:32 a.m. EST and introduced those present, both in person and via teleconference.

Ms. Gallagher then mentioned that the memorandum, *Requirements for Accepting Externally-Issued Identity Credentials*<sup>1</sup>, signed by Steven VanRoekel the U.S. CIO, was sent to the FPKIPA list, and members should be aware of its content and implications. Ms. Gallagher also mentioned that FPKIPA members should be aware of [Executive Order 13587](#) *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information*. The FPKIPA can discuss these at a later date.

### Discuss / Vote on September 13, 2011 FPKIPA Minutes, Matt King

There was a vote to approve the September 13, 2011 FPKIPA minutes. HHS motioned to approve; Postal seconded. The motion was approved unanimously.



Approval Vote for September 13, 2011 FPKIPA Minutes			
Voting members	Vote (HHS Motion; USPS Second)		
	Yes	No	Abstain
Department of Defense (DOD)	Absent		
Department of Energy (DOE)	√		
Department of Health & Human Services (HHS)	√		
Department of Homeland Security (DHS)	√		
Department of Justice (DOJ)	√		
Department of State (State)	√		
Department of the Treasury (Treasury)	Absent		
Drug Enforcement Administration (DEA CSOS)	√		
Government Printing Office (GPO)	√		
General Services Administration (GSA)	√		
National Aeronautics & Space Administration (NASA)	√		
Nuclear Regulatory Commission (NRC)	√		
Social Security Administration (SSA)	Absent		
United States Postal Service (USPS)	√		
United States Patent & Trademark Office (USPTO)	√		
Veterans Administration (VA)	√		

## FPKI Certificate Policy Working Group (CPWG) Report, Charles Froehlich

### 1. Review/Vote on FPKIPA Charter and By-Laws

The CPWG has reviewed and prepared revisions to the FPKIPA Charter and By-Laws that were over a year out of date.

Of greatest concern was the method for choosing a new FPKIPA Chair. The previous version of the Charter called for the bi-annual election of the Chair from the membership; however, this also raised the questions of funding for the Secretariat as well as support for the position (time and funding) by the Chair's parent agency. For these reasons, two versions of the Charter were distributed: one retaining the current method; one changing the method to an appointment by the CIO Council. The revised By-Laws, which outline how the FPKIPA functions, support either version.

Of next greatest concern was the method of designating an alternate to stand in for the Chair when that individual cannot preside at a meeting, or choose to step down early. The CPWG discussed the idea of a Co-Chair, but rejected that idea as overly cumbersome as well as being problematic for the same reasons as choosing a Chair, and opted for the appointment of an alternate by the Chair.

Additional changes included (A) clarification of membership and voting privileges covering all Federal activities; (B) implementation of electronic voting whenever possible; (C) elimination of references to the C4CA and adding references to the SHA-1 FRCA, EGTS, and PIV/PIV-I; (D) recognition of legacy CAs now cross certified with COMMON; and, (E) extension of Charter and By-Laws reviews to a two-year cycle.

The CPWG recommends that the FPKIPA discuss and vote on these documents.

In response to questions, Ms. Gallagher responded that funding for the FPKIPA Secretariat is covered by GSA, and therefore should be taken off the table as part of this discussion; however, resources (time and travel funding) for fulfilling Chair responsibilities would be an agency requirement.

Mr. Toby Slusher commented that with the nomination process still open it might make greater sense to delay any vote on Options A and B until the period ended. Mr. Slusher also indicated that perhaps we should allow the CIO Council to appoint from the list of nominated candidates.

There followed extended discussion with comments from Mr. James Schminky, Mr. David Sulser, Ms. Gallagher, and Mr. Charles Froehlich about the pros and cons of each approach and the rationale used by the CPWG. In the end, it was decided to table the vote on the FPKIPA Charter, but have the CPWG consider a second revision to Option B to have the CIO Council appoint from the list of nominees.

Mr. Froehlich indicated that the CPWG would take this up at their 25 October meeting, and asked for language inputs prior to that meeting. There was then a motion from DoJ, seconded by DoS, to vote to approve the revised FPKIPA By-Laws as written. The revised By-Laws were approved unanimously.

Approval Vote for FPKIPA Bylaws			
Voting members	Vote (DoJ Motion; DoS Second)		
	Yes	No	Abstain
Department of Defense (DOD)	√		
Department of Energy (DOE)	√		
Department of Health & Human Services (HHS)	√		
Department of Homeland Security (DHS)	√		
Department of Justice (DOJ)	√		
Department of State (State)	√		
Department of the Treasury (Treasury)	√		
Drug Enforcement Administration (DEA CSOS)	√		
Government Printing Office (GPO)	√		
General Services Administration (GSA)	√		
National Aeronautics & Space Administration (NASA)	√		
Nuclear Regulatory Commission (NRC)	√		

Social Security Administration (SSA)	Absent		
United States Postal Service (USPS)	√		
United States Patent & Trademark Office (USPTO)	√		
Veterans Administration (VA)	√		

## **ACTION:**

1. At the 25 October meeting, the CPWG will add language to the FPKIPA Charter – Option B indicating that the CIO Council will appoint the FPKIPA Chair from a list of nominees put forward by the FPKIPA membership.

## **2. Discussion/Nominations for FPKIPA Chair**

Discussion on this point necessitated a vote by the FPKIPA on which version of the Charter would be adopted:

- If the FPKIPA adopts Option A to retain the current method for selecting the Chair, the next order of business is to discuss the role of the Chair; the requirements to fill and perform in that position; and to open the floor for nominations.
- If the FPKIPA adopts Option B to pass the responsibility for appointing a Chair to the CIO Council, the only remaining order of business is to discuss the role of the Chair and the requirements to fill and perform in that position so as to advise the CIO Council.

The discussion and nomination for FPKIPA Chair was overcome by the lack of a decision on the FPKIPA Charter. Ms Gallagher indicated that only one nomination had been received so far. The nomination period ends on 31 October 2011. Everyone was encouraged to submit FPKI Chair nominations.

## **3. Review/Vote on FBCA and FCPCA CP LDAP Change Proposals**

Previous questions concerning the LDAP Change Proposals have been resolved. A follow-on discussion was held with NIST about whether LDAP URIs should be optional, and whether AIA and SIA extensions were properly populated. It was suggested that whatever URI is included in certificates must be fully supported. NIST stated that if the language in FIPS 201 could be flexible enough, that would allow the removal of the requirement for LDAP which may solve the problem, and, would take this fact into consideration. NIST also noted that the latest FPKI Certificate Profile makes LDAP optional (but mandatory for SSPs). NIST agreed to send the latest Certificate Profile that makes population of the cDP extension with LDAP URIs optional for Legacy CAs.

Mr. Sulser and Mr. Slusher asked several questions about these change proposals vis-à-vis FIPS 201, which Ms. Wendy Brown and Mr. Froehlich clarified. There was then a motion from HHS, seconded by NRC, to vote to approve both Change Proposals as written. Both Change Proposals were approved unanimously.

Approval Vote for FBCA and FCPCA CP LDAP Change Proposals			
Voting members	Vote (HHS Motion; NRC Second)		
	Yes	No	Abstain
Department of Defense (DOD)	√		
Department of Energy (DOE)	√		
Department of Health & Human Services (HHS)	√		
Department of Homeland Security (DHS)	√		
Department of Justice (DOJ)	√		
Department of State (State)	√		
Department of the Treasury (Treasury)	√		
Drug Enforcement Administration (DEA CSOS)	√		
Government Printing Office (GPO)	√		
General Services Administration (GSA)	√		
National Aeronautics & Space Administration (NASA)	√		
Nuclear Regulatory Commission (NRC)	√		
Social Security Administration (SSA)	Absent		
United States Postal Service (USPS)	√		
United States Patent & Trademark Office (USPTO)	√		
Veterans Administration (VA)	√		

#### 4. Status Update on Device Certificate Change Proposal

At its September 13, 2011 meeting, the FPKIPA adopted the FBCA and Common Policy Change Proposals to implement Device Certificates. Subsequent to that meeting, NIST raised a previously-unforeseen concern regarding the FBCA Change Proposal. Mr. Dave Cooper said we were duplicating verbiage from one proposal to another. It was stated that if there is a problem with duplicate verbiage, we could just remove the language that is duplicated and make references to the requirements in the Common Policy. The CPWG will discuss this issue, and if there are changes to the proposal itself, we will notify the FPKIPA and hold another vote.

#### ACTION:

1. At the 25 October meeting, the CPWG will discuss revising the FBCA Device Change Proposal to address Mr. Cooper's concerns that language in the FBCA change proposal was unnecessary.

## **5. Review/Update Status of CPWG Ongoing Initiatives**

### **a. Review/Update Status of draft Criteria and Methodology**

The CPWG is in the process of reviewing the FBCA Cross Certification Criteria and Methodology document to (A) update it to allow for the various changes that have occurred; (B) incorporate special provisions regarding PIV-I issuers; and, (C) to expand and clarify the requirements for cross certification with other Bridge CAs. The CPWG will continue to review this document at the next CPWG meeting.

### **b. CAB Forum Extend Validation Certificate Guidelines Proposal**

The CPWG has received some comments regarding this document. In short, while the concept of Extended Validation Certificates is a good idea, there are provisions contained in these guidelines that run directly counter to Federal PKI requirements that would make the certificates unacceptable. The question is who is responsible for review and interaction with the CAB Forum—the CPWG, TWG, or the “Dot.Gov” group.

### **c. Definition of CMS**

The CPWG will look at the definition of “CMS” because it is causing problems for state and local governments. We will also look closely at the policies to make sure they are very clear about CMS requirements and how they apply.

## **FPKI Management Authority (FPKIMA) Report, Darlene Gore**

Ms. Darlene Gore asked Ms. Gallagher for Points of Contact (POC) for Mobile trust stores and mobile devices that Ms. Gallagher obtained from the USDA conference. Ms. Brown encouraged everyone to submit POCs if they were working with anyone dealing with mobile trust stores.

The FPKIMA is in the beginning stages of implementing DNSSEC for fpki.gov to provide more security. There should be no impact to those who don't yet support it. Ms. Brown noted that when you resolve the address, the response is signed. Ms. Gallagher pointed out this is another way PKI is used.

The FPKI Incident Management Process document straw man is completed. The document tiger team will be reviewing a second draft at its next (3<sup>rd</sup>) meeting. The tiger team hopes to have a draft for review at the November 3, 2011 CPWG meeting. Ms. Brown summarized the document. The team came up with categories and how to handle different incidents. An incident database will also be developed. Mr. Jim Schminky asked if this will be coordinated with and augment DHS and CERT. Ms. Brown indicated yes, and that is included in the document. Ms. Brown also noted that the document explains more about what happens after notification of an incident (required by policy). Ms. Gallagher stated that this needs to be coordinated with all our partners, vendors, and other stakeholders. Mr. Slusher asked if operational incidents be covered. Mr. Chris Loudon stated that the FPKIMA has its own incident response plan and the current draft focuses on incidents impacting the FPKI Community. Ms. Brown stated that it does not include Problem Management to prevent incidents in the future (i.e., what do you do after incidents have been reported). After an incident is resolved, the associated Problem Management task to identify the cause of the incident and prevent it from happening again may be assigned to the FPKI TWG. This may include developing a white paper, research, developing tests, coordinating with vendors or other FPKI stakeholders.

Ms. Brown mentioned that the FPKI TWG is developing trust store guidance, and will soon be starting a task to test an approach for encryption certificate lookup and retrieval.

An update on TimeStamp paper was given. Microsoft (MS) said that they are not changing their requirements. The FPKIMA is doing more research on this issue, especially the impacts of their response and what is the impact to various agencies if the code signing extended key usage EKU (1.3.6.1.5.5.7.3.3) is not included in the public trust CA listing in the Windows trust store. Mr. Loudon pointed out that MS is working with us on other issues and we now have a dialogue with Microsoft that will allow progress

## **Other Agenda Items**

### **ICAM Updates, Deb Gallagher**

The ICAMSC is next Wednesday in room 701A and B instead of the normal location.

There is new work going on in the ICAMSC, and there are suggestions for additional groups and additional services that may be needed.

We are continuing down the path to include text for PIN caching in FICAM Roadmap and also text about mobile devices – this should also go in FIPS 201.

NIST SP 800-63-1 should be released soon. Language about mobile devices is expected. Ms. Gallagher will send additional information when she can.

As mentioned above, a memo was signed two weeks ago from the Federal CIO requiring acceptance of externally-issued credentials (3<sup>rd</sup>-party credentials) Kantara, InCommon, OIX are approved Trust Framework Providers (TFPs). Others TFPs are coming (e.g., SAFE/BioPharma). What this means is that there may be times when PKI may not be appropriate (or too expensive), so this provides an opportunity for users to use credentials they already have. The key is the credentials need to be issued by TFP-certified Identity Providers. Currently, we don't have any approved level 2 or 3 Identity Providers. Identity Providers are working to figure out how to gather additional information. ICAM is putting together "TFP out of the Box" simple instructions, and there will be a number of meetings to explain how these can be used. There is a timeline for when it is required (e.g., new federal agency applications must accept 3rd party credentials). Ms. Gallagher noted that PIV-I is level 4, and that not all agencies accept PIV-I. The question was asked whether PIV-I providers are automatically an approved provider – it is not clearly stated. Perhaps NIST SP 800-63-1 will clarify (we may need to verify that NIST SP 800-63 is crystal clear on this issue).

Mr. Froehlich noted the new EO 13587 dealing with classified systems. The NSS PKI will publish questions to NSS and any agency operating classified systems asking about what is expected or required from a Common Service Provider. We are looking for comments very soon. If you're running classified systems, the FPKIPA encourage you to look at the EO, since additional security will be required

Ms. Gallagher noted the development of a gap analysis between classified and federal environment to identify what things are missing on either side. Ms. Gallagher hopes to have a draft gap analysis from the ICAMSC.

Ms. Gallagher will be speaking with Verizon about the VA RA Issue (OIG Report). We are working to figure out the best way to address the issue.

The next ICAMSC Meeting is next Wednesday 2011.

The next FPKIPA Meeting is November 8 2011.

**Adjourn Meeting**

Ms. Gallagher adjourned the FPKIPA meeting at 11:19 a.m. EST.

## FPKIPA Action Items

No.	Action Statement	POC	Start Date	Target Date	Status
433	Matt King will place a deadline for C4CA responses for the first August CPWG for all agencies to provide their position on the necessity of the C4CA	Matt King	July 12, 2011	August 8 2011	Closed
434	Ms. Brown will send the MA report to the PA after changing the TWG date.	Wendy Brown	July 12, 2011	July 19, 2011	Closed
435	Ms Cheryl Jenkins will arrange an ad hoc meeting with Microsoft to address the CAPI path validation issues prior to Sept 15, 2011	Cheryl Jenkins	July 12, 2011	September 15, 2011	Closed
436	Ms. Gallagher will send an email with the request for a statement of need for removing the non-revocable certificates to the voting PA members .	Deb Gallagher	July 12, 2011	August 9, 2011	Closed
437	Mr. Matt King will send the EGTS briefing to the group	Matt King	July 12, 2011	August 9, 2011	Closed
438	Ms Gallagher will publish the Digital Signature Guidance once a final review is complete; will be published on the web as well.	Deb Gallagher	July 12, 2011	September 13, 2011	Open
439	Ms. Wendy Brown and Mr. Matt King work to establish a fed-only email list.	Matt King / Wendy Brown	August 9, 2011	September 13, 2011	Open

No.	Action Statement	POC	Start Date	Target Date	Status
442	Mr. King will send ORC PIV-I testing documentation and E-vote to the FPKIPA mail list	Matt King	August 9, 2011	September 13, 2011	Closed
443	Mr. King will send DigiCert audit letter and E-vote to the FPKIPA mail list	Matt King	August 9, 2011	September 13, 2011	Closed
446	The Timestamp Server White Paper will be added to the CPWG and FPKIPA agendas.	FPKIMA	August 9, 2011	September 13, 2011	Closed
449	All FPKIPA members shall submit their nomination for a new FPKIPA Chair to Ms. Gallagher and Mr. King by October 31, 2011	All Voting Members	September 13, 2011	October 31, 2011	Open
450	Ms. Mitchell will provide DoD Lessons Learned from the LDAP transition by Oct 6, 2011.	Debbie Mitchell	September 13, 2011	October 6, 2011	Closed
451	At the 25 October meeting, the CPWG will add language to the FPKIPA Charter – Option B indicating that the CIO Council will appoint the FPKIPA Chair from a list of nominees put forward by the FPKIPA membership	Matt King	October 18, 2011	October 25, 2011	Closed
452	At the 25 October meeting, the CPWG will discuss revising the FBCA Device Change Proposal to address Mr. Cooper's concerns that language in the FBCA change proposal was unnecessary	Matt King	October 18, 2011	October 25, 2011	Closed

